

Helsinki 18.1.2002



ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

CERTIFIED COPY OF
PRIORITY DOCUMENT



Hakija
Applicant

Setec Oy
Vantaa

Patenttihakemus nro
Patent application no

991617

Tekemispäivä
Filing date

16.07.1999

Kansainvälinen luokka
International class

G06K

Keksinnön nimitys
Title of invention

"Menetelmä vasteen tuottamiseksi"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kalla
Tutkimussihteeri

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Menetelmä vasteen tuottamiseksi

Tämän keksintö liittyy ensisijaisesti autentikointilaitteisiin, joiden avulla voidaan autentikoida esimerkiksi toimikortti tai vastaava laite salaiseen avaimeen perustuen. Keksintö liittyy erityisesti salaisen avaimen suojaamiseen siten, että ulkopuolinen hyökkääjä ei pysty selvittämään avainta. Salaista avainta käytetään autentikointioperaatioissa esimerkiksi toimikorttien yhteydessä, jolloin jokaisella toimikortilla on oma yksilöllinen salainen avain, jonka avulla kyseessä olevan toimikortin identiteetti voidaan varmistaa. Esillä oleva keksintö ei kuitenkaan rajoitu yksinomaan toimikortteihin, vaan keksinnön mukaista ratkaisua voidaan hyödyntää myös muissa yhteyksissä, joissa on tarpeen suojata salainen avain. Seuraavassa keksintöä kuitenkin selostetaan esimerkinomaisesti viittaamalla ensisijaisesti toimikortteihin.

Ennestään tunnetaan toimikortti, jolle on järjestetty muisti, esimerkiksi EEPROM muisti, johon on tallennettu salainen avain. Salainen avain muodostuu tyypillisesti bittijonosta, jonka pituus on vähintään 64 bittiä. Toimikortille on lisäksi järjestetty prosessori. Toimikortin identiteetin varmistamiseksi toimikortti kommunikoi ulkopuolisen autentikointiprosessin kanssa, jolloin autentikointiprosessi syöttää toimikortille tietyn syötteen, joka muodostuu bittijonosta. Tällöin toimikortin prosessori hakee muistista sinne etukäteen tallennetun salaisen avaimen, jonka jälkeen prosessori tietyn ennalta määrätyn funktion mukaisesti suorittaa laskuoperaation käyttämällä laskennassa toimikortille syötettyä bittijonoa ja muistista luettua salaista avainta. Laskuoperaation tuloksen, eli vasteen, toimikortti syöttää toimikortin lähdöstä autentikointiprosessille.

Koska autentikointiprosessilla on tiedossa toimikortin salainen avain sekä se funktio, jota toimikortin prosessori käyttää, kykenee se suorittamaan saman laskuoperaation kuin toimikortti. Mikäli autentikointiprosessin suorittaman laskennan tulos vastaa toimikortin lähdöstä saatua tulosta on toimikortin identiteetti varmistettu, koska on olemassa vain yksi ainoa toimikortti, joka sisältää kyseessä olevan salaisen avaimen, ja joka näin ollen vasteena sille syötetylle syötteelle tuottaa kyseessä olevan vasteen.

Edellä selostettuun tunnettuun toimikorttiin liittyy se heikkous, että on olemassa tapoja, jonka avulla ulkopuolinen hyökkääjä voi selvittää toimikortin muistiin tallennetun salaisen avaimen. Eräs tällainen tapa on DPA (Differential Power Analysis), jossa toimikortille toistuvasti (useita tuhansia

kertoja) syötetään erilaisia syötteitä, samalla kun toimikortin lähdöstä saatavaa vastetta, toimikortin laskennan aikana käyttämään virrankulutusta sekä toimikortin laskennan aikana synnyttämää säteilyä seurataan. Syötettä, virrankulutusta, säteilyä ja vastetta tilastoimalla voi ulkopuolinen hyökkääjä saada selville kortin muistiin tallennetun salaisen avaimen. Mikäli hyökkääjä saa selville salaisen avaimen voi hän esimerkiksi kloonata toimikortin, eli valmistaa toisen toimikortin, johon on tallennettu sama salainen avain. Tällaisesta kloonauksesta voi syntyä erittäin suurta haittaa, esimerkiksi jos kyseessä oleva toimikortti on jonkin tietyn henkilön henkilökortti, jonka avulla kyseinen henkilö voidaan elektronisesti identifioida.

Tämä keksinnön tarkoitus on välttää edellä mainittu ongelma, ja saada aikaan ratkaisu, jolla voidaan varmistaa, että ulkopuolinen hyökkääjä ei pysty selvittämään vasteen tuottamisessa käytettävää salaista avainta. Tämä päämäärä saavutetaan keksinnön mukaisella menetelmällä vasteen tuottamiseksi laitteella, joka käsittää: tulo syötteen vastaanottamiseksi, laskinvälineitä syötteelle ja salaiselle avaimelle vasteellisen vasteen tuottamiseksi ensimmäistä ennalta määrättyä laskentafunktiota hyödyntämällä, ja lähdön mainitun vasteen syöttämiseksi edelleen. Keksinnön mukaiselle menetelmälle on tunnusomaista, että tallennetaan laitteen muistiin avainkohtainen luku, ja luetaan mainittu avainkohtainen luku muistista ja suoritetaan ennalta määrättyjä laskuoperaatioita mainitun avainkohtaisen luvun perusteella mainitun vasteen tuottamisen yhteydessä.

Keksinnön kohteena on lisäksi laite, jolla keksinnön mukaista menetelmää voidaan soveltaa. Keksinnön mukaiseen laitteeseen kuuluu: tulo syötteen vastaanottamiseksi, laskinvälineitä syötteelle ja salaiselle avaimelle vasteellisen vasteen tuottamiseksi ensimmäistä ennalta määrättyä laskentafunktiota hyödyntämällä, ja lähtö mainitun vasteen syöttämiseksi edelleen. Keksinnön mukaiselle laitteelle on tunnusomaista, että laite edelleen käsittää: muistin, johon on tallennettu avainkohtainen luku, ja välineitä avainkohtaisen luvun hakemiseksi muistista ja syöttämiseksi laskinvälineille ennalta määrättyjen laskuoperaatioiden suorittamiseksi avainkohtaisen luvun perusteella mainitun vasteen tuottamisen yhteydessä.

Keksinnön kohteena on vielä edelleen järjestelmä, jossa keksinnön mukaista menetelmää ja keksinnön mukaista laitetta voidaan hyödyntää. Keksinnön mukaiseen järjestelmään kuuluu: laite, jossa on tulo syötteen vastaanottamiseksi, laskinvälineitä syötteelle ja salaiselle avaimelle vasteellisen vas-

teen tuottamiseksi ensimmäistä ennalta määrättyä laskentafunktiota hyödyn-
tämällä, ja lähtö mainitun vasteen syöttämiseksi edelleen, ja laitteisto, joka on
kytketty laitteen tuloon, mainitun syötteen syöttämiseksi laitteelle, ja laitteen
lähtöön, mainitun vasteen vastaanottamiseksi, mainitun laitteiston käsittäessä
5 edelleen muistin, johon mainittu salainen avain on tallennettu, laskinvälineitä,
jotka syötteen, salaisen avaimen ja mainitun ensimmäisen ennalta määrätyn
laskentafunktion avulla laskevat tarkistusarvon, ja välineitä, jotka vertaavat
laitteen lähdöstä saatava vastetta tarkistusarvoon, ja jotka osoittavat vastaako
vaste tarkistusarvoa. Keksinnön mukaiselle järjestelmälle on tunnusomaista,
10 että laite edelleen käsittää: muistin, johon on tallennettu avainkohtainen luku, ja
välineitä avainkohtaisen luvun hakemiseksi muistista ja syöttämiseksi laskinväli-
neille ennalta määrättyjen laskuoperaatioiden suorittamiseksi avainkohtaisen
luvun perusteella mainitun vasteen tuottamisen yhteydessä.

Keksintö perustuu siihen ajatukseen, että vasteen tuottamiseen
15 käytettävän salaisen avaimen selvittäminen vaikeutuu huomattavasti, kun
vasteen tuottamisen yhteydessä luetaan laitteen muistista avainkohtainen lu-
ku, jota hyödynnetään ennalta määrättyjen laskuoperaatioiden suorittamiseen
vasteen tuottamisen yhteydessä. Tällöin nimittäin laitteen vasteen tuottami-
seen käyttämä virrankulutus ja säteily ei enää riipu yksinomaan salaisesta
20 avaimesta, syöttestä ja laskennassa käytettävästä funktiosta, vaan myös
avainkohtaisen luvun käsittely aiheuttaa tietyn mitattavan virrankulutuksen ja
säteilyn, joka entisestään vaikeuttaa salaisen avaimen selvittämistä. Ulkopuo-
linen hyökkääjä ei voi tällöin varmuudella tietää mikä osa mitattavissa olevasta
virrankulutuksesta ja säteilystä on aiheutunut avainkohtaisen luvun käsittelystä
25 ja mikä osa taas vuorostaan varsinaisesta vasteen tuottamisesta.

Sen sijaan, että laitteen laskinvälineet hyödyntävät erillistä laskenta-
funktiota ja erillistä salaista avainta on myös ajateltavissa, että salainen avain
on käytettävän laskentafunktion osa. Tällöin esimerkiksi salaisen avaimen
muuttaminen itse asiassa merkitsee, että laitekohtaista laskentafunktiota
30 muutetaan, ja vastaavasti salaisen avaimen selvittäminen merkitsee itse asi-
assa, että salainen laitekohtainen funktio selvitetään.

Avainkohtaisella luvulla tarkoitetaan sellaista lukua, joka on käytös-
sä olennaisesti koko avaimen käyttöänsä ajan. Eli silloin kun salainen avain
vaihdetaan, vaihdetaan myös avainkohtainen luku. Avainkohtainen luku voi
35 muodostua esimerkiksi satunnaisluvusta, jonka satunnaislukugeneraattori
tuottaa uuden salaisen avaimen käyttöönoton yhteydessä. Vaihtoehtoisesti

avainkohtainen luku voi muodostua esimerkiksi pseudo-satunnaisluvusta. Tärkeää on kuitenkin se, että jo käytössä olutta avainkohtaista lukua ei oteta kovin usein uudelleen käyttöön.

- Keksinnön mukaisen ratkaisun merkittävin etu on näin ollen se, että
- 5 ulkopuolisen hyökkääjän on entistä hankalampi selvittää vasteen tuottamisessa käytetty salainen avain, koska esimerkiksi laitteen virrankulutus ja säteily ei enää anna oikeaa kuvaa vasteen tuottamisen aiheuttamasta todellisesta virrankulutuksesta ja säteilystä, jolloin edes tilastollisilla menetelmillä ei enää pystytä selvittämään käytössä olevaa salaista avainta.
 - 10 Eräässä keksinnön mukaisen laitteen edullisessa suoritusmuodossa salainen avain on tallennettu laitteen muistiin, josta se voidaan hakea laskeviin välineen käyttöön vasteen tuottamisen yhteydessä. Tällöin myös avainkohtainen luku on tallennettu laitteen muistiin. Vasteen tuottamisen yhteydessä muistista haetaan näin ollen sekä salainen avain, että avainkohtainen luku.
 - 15 Salaista avainta käytetään tämän jälkeen vasteen tuottamiseen, samalla kun avainkohtaisella luvulla suoritetaan ennalta määrättyä laskentaa, joka ei vaikuta tuotettavaan vasteeseen. Näin ollen laitteen virrankulutus ja säteily saadaan näyttämään toiselta, kuin mitä vasteen tuottaminen itse asiassa edellyttäisi.
 - 20 Eräässä keksinnön mukaisen laitteen toisessa edullisessa suoritusmuodossa salaista avainta ei ole tallennettu lainkaan laitteen muistiin. Sen sijaan salainen avain on koodattu käyttämällä toista ennalta määrättyä laskentafunktiota sekä avainkohtaista lukua. Tällöin koodattu avain sekä avainkohtainen luku on tallennettu laitteen muistiin. Vasteen tuottamisen yhteydessä
 - 25 laitteen muistista luetaan koodattu avain sekä avainkohtainen luku, jonka jälkeen toisen laskentafunktion käänteisfunktion avulla lasketaan salainen avain, jota käytetään vasteen tuottamisessa. Tällöin salaisen avaimen laskennasta aiheutuva säteily ja virrankulutus estää ulkopuolista hyökkääjää selvittämästä vasteen tuottamisen yhteydessä syntyvää säteilyä ja virrankulutusta. Lisäksi
 - 30 avainta ei tässä suoritusmuodossa ole tallennettu lainkaan laitteen muistiin. Tunnetuissa ratkaisuissa on osoittautunut, että nimenomaan salaisen avaimen lukeminen muistista on sellainen operaatio, joka antaa ulkopuoliselle hyökkääjälle erityisen paljon informaatiota.
 - 35 Eräässä keksinnön mukaisen laitteen kolmannessa edullisessa suoritusmuodossa laite käsittää välineitä, joilla se määrävälein, esimerkiksi kun laite on tuottanut 1000 vastetta, laskee uuden koodatun avaimen uuden

avainkohtaisen luvun ja toisen ennalta määrätyn funktion avulla. Kyseisen uuden koodatun avaimen ja uuden avainkohtaisen luvun laite tallentaa muistiinsa aikaisempien tilalle. Tämä keksinnön mukainen suoritusmuoto vaikeuttaa entisestään salaisen avaimen selvittämistä, koska ulkopuolinen hyökkääjä kykenee tällöin tilastoimaan säteilyä ja virrankulutusta esimerkiksi vain mainitun 1000 vasteen tuottamisen ajan, jonka jälkeen tapahtuu olennainen muutos vasteen tuottamisen yhteydessä suoritettavissa laskentaoperaatioissa, minkä vuoksi tilastoinnista ei ole hyötyä.

Keksinnön mukaisen menetelmän, laitteen ja järjestelmän edulliset suoritusmuodot ilmenevät oheisista epäitsenäisistä patenttivaatimuksista 2 - 5, 7 - 9 ja 11 -13.

Keksintöä selostetaan seuraavassa esimerkinomaisesti lähemmin viittaamalla oheisiin kuvioihin, joista:

kuvio 1 esittää vuokaaviota keksinnön mukaisen menetelmän ensimmäisestä edullisesta suoritusmuodosta,

kuvio 2 esittää lohkokaaaviota keksinnön mukaisen laitteen ensimmäisestä edullisesta suoritusmuodosta,

kuvio 3 esittää lohkokaaaviota keksinnön mukaisen laitteen toisesta edullisesta suoritusmuodosta,

kuvio 4 esittää lohkokaaaviota keksinnön mukaisen laitteen kolmannelta edullisesta suoritusmuodosta,

kuvio 5 esittää lohkokaaaviota keksinnön mukaisen järjestelmän ensimmäisestä edullisesta suoritusmuodosta, ja

kuvio 6 esittää lohkokaaaviota keksinnön mukaisen järjestelmän toisesta edullisesta suoritusmuodosta.

Kuvion 1 vuokaaviota voidaan hyödyntää esimerkiksi toimikortin autentikointiin, eli sen avulla voidaan varmistaa, että kyseessä on toimikortti, joka vasteena sille syötetylle syötteelle todella tuottaa ennalta määrätyn vasteen, jonka arvo on riippuvainen salaisesta avaimesta, joka on toimikorttikohmainen. Toimikorttikohtaisella salaisella avaimella tarkoitetaan, että käytössä olevista toimikorteista ainoastaan yksi ainoa käyttää kyseistä salaista avainta vasteen tuottamisessa.

Kuvion 1 lohossa A laitteelle, eli toimikortille, syötetään tietty syöte INPUT. Kyseinen syöte muodostuu käytännössä bittijonosta, jolla on ennalta määrätty pituus.

Lohkossa B haetaan laitteen muistiin tallennettu avainkohtainen luku RND. Kyseessä voi olla esimerkiksi satunnaisluku, joka on määritelty ja tallennettu laitteen muistiin samanaikaisesti kun toimikortille on määritelty salainen avain.

- 5 Lohkossa C lasketaan ensimmäistä funktiota f hyödyntävillä laskinvälineillä salaisen avaimen A ja syöteen INPUT perusteella vaste OUTPUT. Vasteen laskennan yhteydessä suoritetaan lisäksi ennalta määrättyjä laskuoperaatioita lohkoissa B luetun avainkohtaisen luvun RND perusteella.

- 10 Mikäli salainen avain A on tallennettu laitteen muistiin, ovat avainkohtaiseen lukuun RND liittyvät laskuoperaatiot sellaisia, että ne eivät vaikuta laskinvälineiden laskemaan vasteeseen OUTPUT. Eli tässä tapauksessa käytetään jotakin sopivaksi katsottua laskentakaava, jolloin laskennasta aiheutuva energiankulutus ja säteily ainoastaan vääristävät laitteen kokonaisenergiankulutusta ja kokonaissäteilyä vasteen tuottamisen yhteydessä.

- 15 Mikäli sitävastoin salaista avainta A ei ole tallennettu laitteen muistiin, vaan sen sijan laitteen muistiin on tallennettu avainkohtaisen luvun RND lisäksi koodattu avain A' , joka on laskettu salaista avainta A , avainkohtaista lukua RND ja toista ennalta määrättyä funktiota g hyödyntämällä (eli $A'=g(\text{RND}, A)$), ovat avainkohtaiseen lukuun RND liittyvät laskuoperaatiot sellaisia, että niiden tuloksena saadaan salainen avain A . Tällöin käytetään mainitun toisen ennalta määrätyn funktion g käänteisfunktiota g' , jonka avulla salainen avain A voidaan laskea avainkohtaisen luvun RND ja koodatun avaimen A' perusteella (eli $A=g'(\text{RND}, A')$). Tällöin avaimen A laskemiseen kulunut energia ja siitä syntynyt säteily vääristää sitä kokonaisenergiankulutusta ja
- 20 kokonaissäteilyä, joka syntyy vasteen OUTPUT tuottamisesta

- Lohkossa D syötetään vaste OUTPUT laitteen lähdöstä. Vasteen perusteella esimerkiksi ulkopuolinen autentikointilaitteisto voi varmistaa, että kyseessä on oikea toimikortti. Tämä tapahtuu siten, että autentikointilaitteisto, jolla on tiedossa funktio f , salainen avain A ja syöte INPUT suorittaa vastaavan laskuoperaation kuin toimikortti. Tällöin toimikortin tuottama vasteen OUTPUT tulisi olla sama kuin autentikointilaitteiston suorittaman laskuoperaation tulos.
- 30

- Kuvio 2 esittää lohkokaaaviota keksinnön mukaisen laitteen ensimmäisestä edullisesta suoritusmuodosta. Kuviossa 2 oleva laite voi olla esimerkiksi henkilökortti, jonka avulla henkilön henkilöllisyys voidaan elektronisesti varmentaa, elektroninen maksukortti, jonka muistiin on tallennettu tietty rahasaldo, lupakortti, joka osoittaa televisiovastaanottoon kytkeytylle satelliitti-
- 35

vastaanottimelle, että tietyn maksullisen kanavan katseleminen on sallittua, tai mikä tahansa muu laite, jonka luotettava autentikointi on tarpeen.

Laitteeseen 1 kuuluu prosessorista P muodostuva laskinväline, joka hyödyntää tiettyä laskentafunktiota f . Laitteeseen 1 kuuluu lisäksi muisti M, joka voi olla esimerkiksi EEPROM muisti. Muistiin M on tallennettu laitteen 1 salainen avain A, joka muodostuu bittijonosta, jonka pituus voi olla esimerkiksi 64 bittiä. Muistiin M on lisäksi tallennettu avainkohtainen luku RND, joka myös muodostuu bittijonosta.

Kun laitteen 1 tuloon 2 syötetään tietty syöte INPUT hakee prosessori P muistista M sinne tallennetun salaisen avaimen A ja avainkohtaisen luvun RND. Tämän jälkeen prosessori P laskee ensimmäisen ennalta määrätyn laskentafunktion f avulla vasteen OUTPUT, jonka arvo riippuu salaisesta avaimesta A ja syötteestä INPUT, eli $OUTPUT=f(INPUT, A)$. Vasteen OUTPUT laskennan yhteydessä prosessori P suorittaa laskentaa myös laskentafunktiota f_2 sekä avainkohtaista lukua RND hyödyntämällä. Laskentafunktion f_2 avulla tehdyt laskut eivät vaikuta prosessorin tuottamaan vasteeseen OUTPUT, mutta sitävastoin laskentaan käytetty energiankulutus ja laskennan aiheuttama säteily muuttuu, jolloin ulkopuolisen hyökkääjän on mahdoton selvittää vasteen OUTPUT tuottamiseen tarvittu energia sekä siitä syntynyt säteily.

Kuvion 2 tapauksesta poiketen on myös mahdollista, että laitteeseen 1 kuuluu kaksi prosessoria, joista toinen suorittaa laskuja funktion f perusteella, ja toinen funktion f_2 perusteella.

Kun prosessori P on kuvion 2 tapauksessa suorittanut sekä laskentafunktiolla f että f_2 suoritettavat laskut loppuun, syöttää se laskentafunktiolla f syntyneen vasteen OUTPUT laitteen 1 lähdölle 3, josta esimerkiksi ulkopuolinen autentikointiprosessi voi sen lukea.

Kuvio 3 esittää lohkokaaaviota keksinnön mukaisen laitteen toisesta edullisesta suoritusmuodosta. Kuvion 3 suoritusmuoto vastaa hyvin pitkälle kuvion 2 suoritusmuotoa. Kuvion 3 tapauksessa kuitenkin muistiin M' on salaisen avaimen A sijasta tallennettu koodattu avain A'. Näin ollen laitteeseen 1' ei lainkaan ole tallennettu salaista avainta A, jolloin myös vältytään siltä, että salainen avain jossain vaiheessa olisi luettava muistista. Nimenomaan salaisen avaimen lukeminen muistista on sellainen toimenpide, joka antaa erityisen paljon informaatiota ulkopuoliselle hyökkääjälle, joka pyrkii selvittämään laitteen salaisen avaimen.

Kuvion 3 tapauksessa laitteen 1' muistiin M' on tallennettu koodattu avain A' sekä avainkohtainen luku RND. Koodattu avain A' on muodostettu salaisen avaimen A ja avainkohtaisen luvun RND sekä toisen ennalta määrätyn funktion g avulla siten, että $A'=g(A, RND)$.

- 5 Kun prosessori P' vastaanottaa laitteen 1' tulon 2 kautta syötetyn syötteen INPUT, hakee se muistista M' koodatun avaimen A' ja avainkohtaisen luvun RND. Tämän jälkeen prosessori P' hyödyntää muistista haettuja bittijonoja A' ja RND toisen ennalta määrätyn funktion g käänteisfunktion g' perusteella suoritettavissa laskuoperaatioissa. Näiden laskuoperaatioiden tuloksena
- 10 prosessori P' saa selville salaisen avaimen, eli $A=g'(A',RND)$.

Kun salainen avain A on prosessorin tiedossa hyödyntää se sitä ensimmäisen ennalta määrätyn funktion f perusteella suoritettavissa laskuissa, joiden tuloksena syntyy vaste OUTPUT, eli $OUTPUT=f(INPUT,A)$.

- Sillä, että salainen avain lasketaan koodatusta avaimesta ja avainkohtaisesta luvusta, saavutetaan se etu, että laitteen 1' vasteen tuottamiseen käyttämä energia ja siitä syntynyt säteily näyttää suuremmalta tai pienemmältä kuin mitä se todellisuudessa on. Ulkopuolinen hyökkääjä ei voi selvittää varsinaista vasteen OUTPUT tuottamiseen kulunutta energiaa ja siitä aiheutunutta säteilyä muusta energiankulutuksesta ja säteilystä.
- 15

- 20 Kuvion 3 tapauksesta poiketen on luonnollisesti mahdollista, että laitteessa on kaksi prosessoria, joista toinen suorittaa funktiolla g' suoritettavat laskut, ja toinen funktiolla f suoritettavat laskut.

- Kuvio 4 esittää lohkokaaaviota keksinnön mukaisen laitteen kolmannesta edullisesta suoritusmuodosta. Kuvion 4 suoritusmuoto vastaa hyvin pitkälle kuvion 3 suoritusmuotoa. Kuvion 4 tapauksessa laitteeseen 1" kuuluu kuitenkin välineitä uuden koodatun avaimen A' ja uuden avainkohtaisen luvun RND käyttöön ottamiseksi.
- 25

- Kuvion 4 tapauksessa prosessoriin P" kuuluu laskuri, joka pitää kirjaa siitä, miten monta kertaa prosessori P" on tuottanut vasteen OUTPUT. Kun kyseinen laskuri saavuttaa ennalta määrätyn raja-arvon, esimerkiksi 1000, käynnistää prosessori P" prosessin uuden koodatun avaimen A' ja uuden avainkohtaisen luvun RND käyttöön ottamiseksi. Tällöin prosessori P" laskee salaisen avaimen A muistiin M" tallennetun koodatun avaimen A', avainkohtaisen luvun RND sekä laskentafunktion g' perusteella. Näin lasketun salaisen avaimen A prosessori P" syöttää toiselle prosessorille 5" (kuvion 4 esimerkistä poiketen laitteessa 1" voi myös olla yksi ainoa prosessori, jolloin kuvion 4 pro-
- 30
- 35

essori P" suorittaa myös kuvion 4 toisen prosessorin 5" toiminnot). Samalla prosessori P" ohjaa satunnaislukugeneraattoria 4" tuottamaan uuden satunnaisluvun, jonka satunnaislukugeneraattori syöttää toiselle prosessorille 5".

Toinen prosessori 5" on ohjelmoitu suorittamaan laskentaa toisen
 5 ennalta määrätyn laskentafunktion g avulla. Näin ollen se laskee salaisen avaimen A ja uuden satunnaisluvun RND perusteella uuden koodatun avaimen A', jolloin $A' = g(A, RND)$. Kyseisen uuden koodatun avaimen A' prosessori 5" tallentaa yhdessä satunnaisluvusta muodostuvan uuden avainkohtaisen luvun RND kanssa muistiin M", aikaisemman koodatun avaimen ja aikaisemman avainkohtaisen koodin tilalle.
 10

Lopuksi prosessori P" nollaa laskurin, jolloin laite 1" jatkossa hyödyntää uutta koodattua avainta sekä uutta avainkohtaista lukua, kunnes laskuri jälleen osoittaa, että prosessori P" on tuottanut raja-arvoa (esim. 1000) vastaavan lukumäärän vasteita OUTPUT, jolloin jälleen käynnistyy uuden koodatun avaimen laskenta.
 15

Kuvio 5 esittää lohkokaaviota keksinnön mukaisen järjestelmän ensimmäisestä edullisesta suoritusmuodosta. Kuviossa 5 esitetyssä järjestelmässä hyödynnetään kuvion 2 yhteydessä selostettua laitetta 1.

Laite 1 on kytketty laitteistoon 10, joka voi olla esimerkiksi autentikointilaitteisto. Laitetta 1 ja laitteistoa 10 ei tarvitse fyysisesti kytkeä toisiinsa, vaan laitteisto 10 voi olla esimerkiksi tietokonelaitteisto, joka Internetin tai jonkin toisen tietoverkon välityksellä on tiedonsiirtoyhteydessä laitteeseen 1. Jos laite 1 on elektroninen henkilökortti, joka on asetettu Internet-verkkoon kytkeytyn tietokoneen kortinlukijaan, voi laitteisto 10 Internetin ja laitteen 1 välityksellä varmistua siitä, kuka kyseisellä hetkellä käyttää tietokonetta, jolloin oletetaan että kyseessä on se henkilö, jonka henkilökortti kyseisellä hetkellä on asetettu lukijaan.
 20
 25

Laitteistoon 10 kuuluu muisti M2, johon on tallennettu kaikkien käytössä olevien laitteiden (henkilökorttien) salaiset avaimet. Kun laitteisto näin ollen haluaa varmistaa, että kyseessä on tietty laite 1, hakee se kyseisen laitteen 1 salaisen avaimen A muististaan M2 autentikointia varten. Tällöin myös laitteiston 10 ohjausyksikkö 11 tuottaa ennalta määrätyn syötteen INPUT. Kyseisen syötteen ohjausyksikkö 11 lähettää sekä laitteelle 1, että laitteiston prosessorille P2. Laitteiston prosessori P2 käyttää samaa laskentafunktiota f kuin laitteen 1 prosessori P. Koska molemmat prosessorit käyttävät
 30
 35 samaa laskentafunktiota f, sama salaista avainta A ja sama syötettä INPUT

tulisi myös niiden tuottama vaste OUTPUT olla sama. Tämän varmistamiseksi laitteistoon kuuluu vertailuväline 12, joka vertaa laitteen lähdöstä 3 saatavaa vastetta prosessorin P2 tuottamaan vasteeseen, ja vertailun perusteella esimerkiksi tuottaa signaalin, joka kuvaa vertailun tulosta.

- 5 Laitteistoa 10 voidaan lisäksi käyttää laitteen 1 salaisen avaimen muuttamiseksi. Tällöin laitteiston ohjausyksikkö 11 generoi uuden salaisen avaimen A, jonka se tallentaa muistiin M2 sekä lähettää laitteistolle 1. Uuden salaisen avaimen A generoinnin yhteydessä laitteiston 10 satunnaislukugeneraattori 13 tuottaa lisäksi uuden avainkohtaisen luvun RND, jonka laitteisto
10 myös lähettää laitteelle 1. Laite 1 vastaanottaa näin uuden salaisen avaimen A ja uuden avainkohtaisen luvun RND, jotka se tallentaa aikaisempien tilalle muistiin M.

- Kuvio 6 esittää lohkokaaaviota keksinnön mukaisen järjestelmän toisesta edullisesta suoritusmuodosta. Kuvion 6 suoritusmuoto vastaa hyvin pitkälle kuvion 5 suoritusmuotoa.
15

Kuvion 6 suoritusmuodossa laitteisto 10' ei kuitenkaan lähetä uutta salaista avainta A tallennettavaksi laitteen 1' muistiin. Sen sijaan uusi salainen avain A ja satunnaislukugeneraattorin 13 tuottama uusi avainkohtainen luku syötetään prosessorille 14. Salainen avain A tallennetaan lisäksi muistiin M2.

- 20 Prossessori 14 laskee toista ennalta määrättyä laskentafunktiota g ja avainkohtaista lukua hyödyntämällä koodatun avaimen A' . Tällöin $A'=g(RND, A)$. Tämän jälkeen laitteisto 10' lähettää uuden koodatun avaimen A' ja avainkohtaisen luvun RND laitteelle 1', joka tallentaa ne muistiin M'. Kyseistä koodattua avainta A' ja avainkohtaista lukua RND laite 1' käyttää kuten kuvion 3 yhteydessä on selostettu.
25

- On ymmärrettävä, että edellä oleva selitys ja siihen liittyvät kuviot on ainoastaan tarkoitettu havainnollistamaan esillä olevaa keksintöä. Alan ammattimiehelle tulevat olemaan ilmeisiä erilaiset keksinnön variaatiot ja muunnelmat ilman että poiketaan oheisissa patenttivaatimuksissa esitetyn
30 keksinnön suojapiiristä ja hengestä.

Patenttivaatimukset:

1. Menetelmä vasteen tuottamiseksi laitteella, joka käsittää:
tulon (2) syötteen (INPUT) vastaanottamiseksi,
5 laskinvälineitä (P, P', P'') syötteelle ja salaiselle avaimelle (A) vasteellisen vasteen (OUTPUT) tuottamiseksi ensimmäistä ennalta määrättyä laskentafunktiota (f) hyödyntämällä, ja
lähdön (3) mainitun vasteen (OUTPUT) syöttämiseksi edelleen,
tunnettu siitä, että
10 tallennetaan laitteen muistiin (M, M', M'') avainkohtainen luku (RND),
ja
luetaan mainittu avainkohtainen luku (RND) muistista ja suoritetaan ennalta määrättyjä laskuoperaatioita mainitun avainkohtaisen luvun perusteella mainitun vasteen (OUTPUT) tuottamisen yhteydessä.
- 15 2. Patenttivaatimuksen 1 mukainen menetelmä, tunnettu siitä, että mainittu salainen avain (A) on tallennettu laitteen (1) muistiin (M).
3. Patenttivaatimuksen 1 mukainen menetelmä, tunnettu siitä, että
laitteen (1', 1'') muistiin (M', M'') on tallennettu salaisen avaimen
20 (A), avainkohtaisen luvun (RND) sekä toisen ennalta määrätyn laskentafunktion (g) avulla laskettu koodattu avain (A'), ja että
vasteen (OUTPUT) tuottamisen yhteydessä suoritettavalla ennalta määrättyllä laskuoperaatiolla lasketaan mainitun avainkohtaisen luvun (RND) ja muistiin tallennetun koodatun avaimen (A') perusteella salainen avain (A)
25 käyttämällä mainitun toisen ennalta määrätyn laskentafunktion (g) käänteisfunktioita (g'), ja
hyödynnetään laskettua salaista avainta (A) mainitun vasteen (OUTPUT) tuottamisessa.
4. Patenttivaatimuksen 3 mukainen menetelmä, tunnettu
30 siitä, että mainittu toinen ennalta määrätty funktio (g) on laitekohtainen funktio, ja että mainittu avainkohtainen luku (RND) on satunnaisluku.
5. Jonkin patenttivaatimuksen 2 - 4 mukainen menetelmä, tunnettu siitä, että lasketaan ja tallennetaan laitteen (1'') muistiin (M'') uusi koodattu avain (A') sekä uusi avainkohtainen luku (RND), kun laskinvälineet
35 (P'') ovat hyödyntäneet mainittua ensimmäistä ennalta määrättyä funktiota (f) ennalta määrätyn monta kertaa.

6. Laite (1, 1', 1''), johon kuuluu:
 tulo syötteen vastaanottamiseksi,
 laskinvälineitä (P, P', P'') syötteelle (INPUT) ja salaiselle avaimelle
 (A) vasteellisen vasteen (OUTPUT) tuottamiseksi ensimmäistä ennalta mää-
 5 rättyä laskentafunktiota (f) hyödyntämällä, ja
 lähtö (3) mainitun vasteen (OUPUT) syöttämiseksi edelleen, t u n -
 n e t t u s i i t ä , että laite edelleen käsittää:
 muistin (M, M', M''), johon on tallennettu avainkohtainen luku (RND),
 ja
 10 välineitä avainkohtaisen luvun (RND) hakemiseksi muistista (M, M',
 M'') ja syöttämiseksi laskinvälineille (P, P', P'') ennalta määrättyjen laskuoperaa-
 tioiden (f2, g') suorittamiseksi avainkohtaisen luvun (RND) perusteella mainitun
 vasteen (OUPUT) tuottamisen yhteydessä.

7. Patenttivaatimuksen 6 mukainen laite, t u n n e t t u s i i t ä , että
 15 mainittu salainen avain (A) on tallennettu laitteen (1) muistiin (M').

8. Patenttivaatimuksen 6 mukainen laite, t u n n e t t u s i i t ä ;
 että mainitun laitteen (1', 1'') muistiin (M', M'') on tallennettu koodattu
 avain (A'), joka on laskettu salaisen avaimen (A), avainkohtaisen luvun (RND)
 sekä toisen ennalta määrätyn laskentafunktion (g) avulla, ja
 20 että laskinvälineiden (P', P'') mainittuihin ennalta määrättyihin las-
 kuoperaatioihin sisältyy salaisen avaimen (A) laskeminen muistiin (M', M'') tal-
 lennetun koodatun avaimen (A'), avainkohtaisen luvun (RND) sekä mainitun
 toisen ennalta määrätyn laskentafunktion (g) käänteisfunktion (g') avulla maini-
 tun vasteen (OUTPUT) tuottamisen yhteydessä.

9. Patenttivaatimuksen 8 mukainen laite, t u n n e t t u s i i t ä , että
 25 laite (1'') käsittää koodausvälineitä (5'') uuden salaisen avaimen (A') laskemisek-
 si salaisen avaimen (A), koodausvälineille syötettävän uuden avainkohtaisen
 luvun (RND) ja mainitun toisen ennalta määrätyn laskentafunktion (g) avulla, ja
 että laite (1'') käsittää välineitä muistiin (M'') tallennetun koodatun avaimen (A') ja
 30 avainkohtaisen luvun (RND) korvaamiseksi koodausvälineiden (5'') laskemalla
 uudella koodatulla avaimella (A') ja uudella avainkohtaisella koodilla (RND).

10. Järjestelmä, johon kuuluu:
 laite (1, 1', 1''), jossa on tulo syötteen (INPUT) vastaanottamiseksi,
 laskinvälineitä (P, P', P'') syötteelle (INPUT) ja salaiselle avaimelle (A) vasteel-
 35 lisen vasteen (OUTPUT) tuottamiseksi ensimmäistä ennalta määrättyä las-

kentäfunktiota (f) hyödyntämällä, ja lähtö mainitun vasteen syöttämiseksi edelleen, ja

5 laitteisto (10, 10'), joka on kytketty laitteen (1, 1', 1'') tuloon, mainitun syötteen (INPUT) syöttämiseksi laitteelle, ja laitteen lähtöön, mainitun vasteen (OUTPUT) vastaanottamiseksi, mainitun laitteiston (10, 10') käsittäessä edelleen muistin (M2), johon mainittu salainen avain (A) on tallennettu, laskinvälineitä (P2), jotka syötteen (INPUT), salaisen avaimen (A) ja mainitun ensimmäisen ennalta määrätyn laskentafunktion (f) avulla laskevat tarkistusarvon, ja välineitä (12), jotka vertaavat laitteen (1) lähdöstä saatava vastetta 10 (OUTPUT) tarkistusarvoon, ja jotka osoittavat vastaako vaste tarkistusarvoa, tunnettu siitä, että laite (1, 1', 1'') edelleen käsittää:

muistin (M, M', M''), johon on tallennettu avainkohtainen luku (RND), ja

15 välineitä avainkohtaisen luvun (RND) hakemiseksi muistista ja syöttämiseksi laskinvälineille (P, P', P'') ennalta määrättyjen laskuoperaatioiden suorittamiseksi avainkohtaisen luvun (RND) perusteella mainitun vasteen tuottamisen yhteydessä.

11. Patenttivaatimuksen 10 mukainen järjestelmä, tunnettu siitä, että mainittu laitteisto (10) käsittää välineitä salaisen avaimen (A) sekä 20 avainkohtaisen luvun (RND) tallentamiseksi laitteen (1) muistiin (M).

12. Patenttivaatimuksen 10 mukainen järjestelmä, tunnettu siitä, että mainittu laitteisto (10') käsittää

25 välineitä koodatun avaimen (A') laskemiseksi salaisen avaimen (A), avainkohtaisen luvun (RND) ja toisen ennalta määrätyn laskentafunktion (g) avulla, ja

välineitä koodatun avaimen (A') ja avainkohtaisen luvun (RND) tallentamiseksi laitteen (1') muistiin (M').

13. Patenttivaatimuksen 12 mukainen järjestelmä, tunnettu siitä, että mainittu laitteisto (10') edelleen käsittää satunnaislukugeneraattorin 30 (13) avainkohtaisen luvun (RND) tuottamiseksi koodatun avaimen (A') laskennan yhteydessä.

(57) Tiivistelmä

Tämän keksinnön kohteena on laite (1), johon kuuluu: tulo syötteen vastaanottamiseksi, laskinvälineitä (P) syötteelle (INPUT) ja salaiselle avaimelle (A) vasteellisen vasteen (OUTPUT) tuottamiseksi ensimmäistä ennalta määrättyä laskentafunktiota (f) hyödyntämällä, ja lähtö (3) mainitun vasteen (OUPUT) syöttämiseksi edelleen. Jotta ulkopuolinen hyökkääjä ei voisi selvittää salaista avainta käsittää laite edelleen: muistin (M), johon on tallennettu avainkohtainen luku (RND), ja välineitä avainkohtaisen luvun (RND) hakemiseksi muistista (M) ja syöttämiseksi laskinvälineille (P') ennalta määrättyjen laskuoperaatioiden (f2) suorittamiseksi avainkohtaisen luvun (RND) perusteella mainitun vasteen (OUPUT) tuottamisen yhteydessä.

Kuvio 2

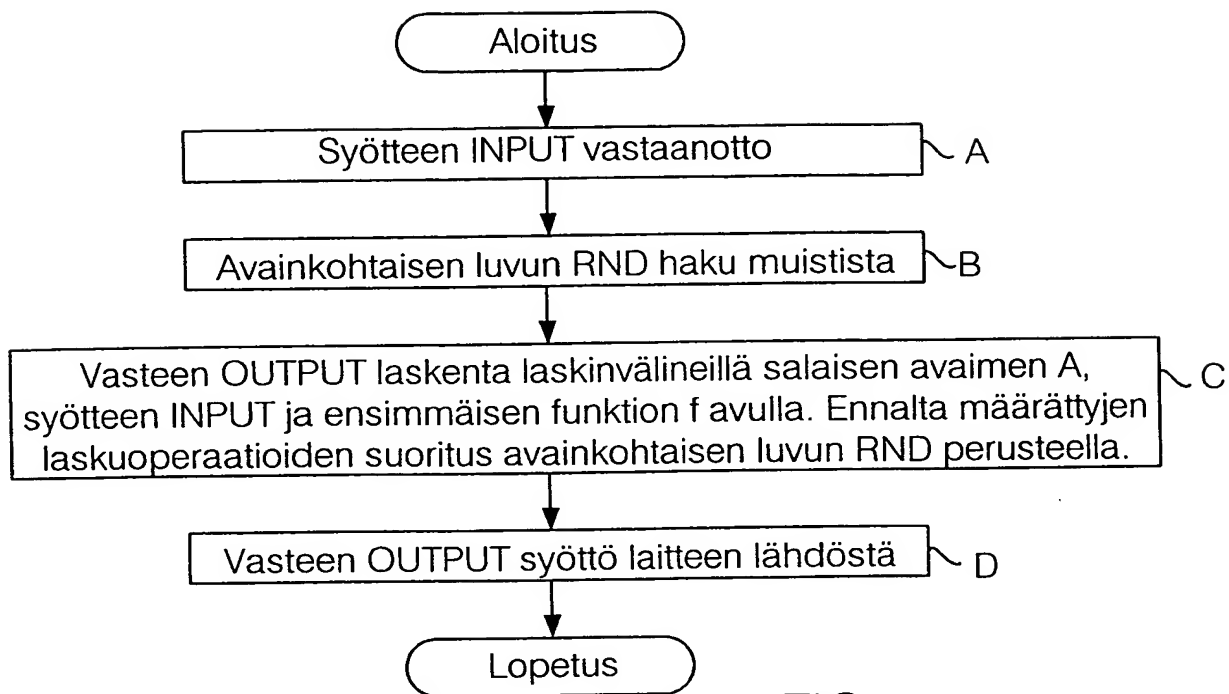


FIG. 1

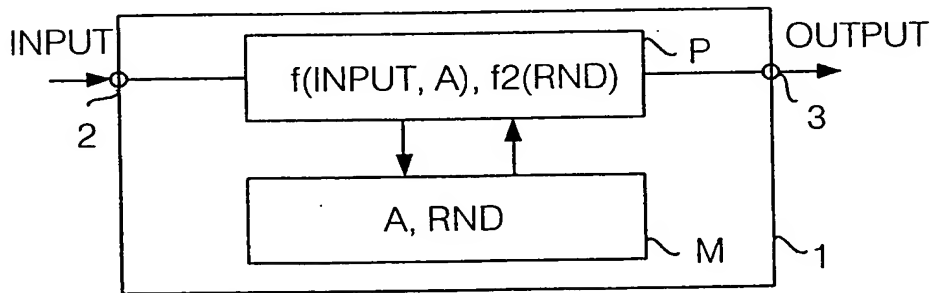


FIG. 2

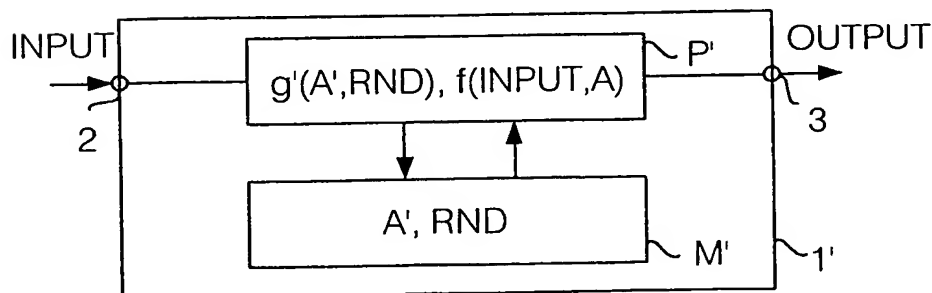


FIG. 3

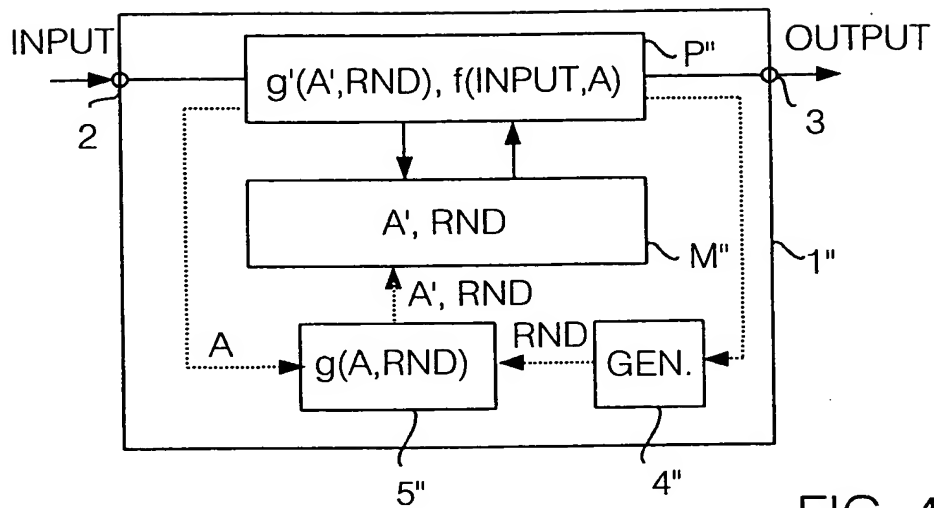


FIG. 4

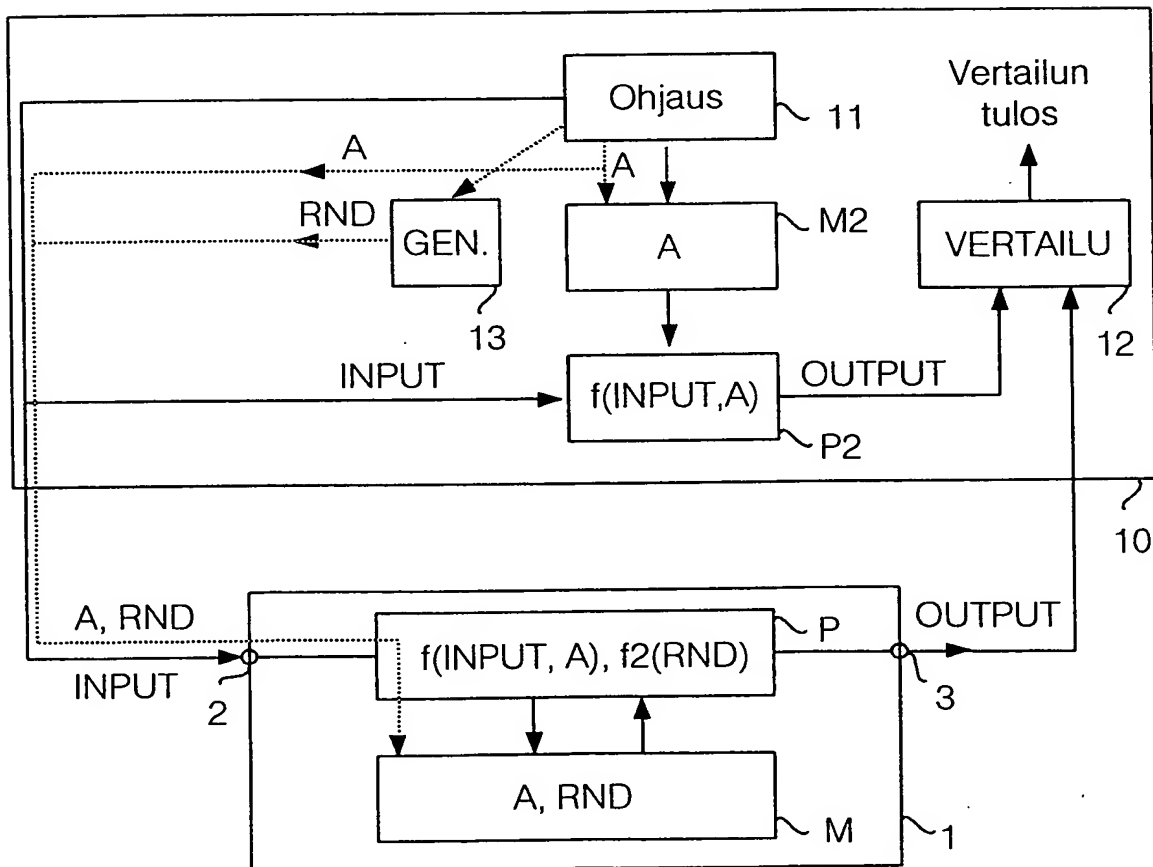


FIG. 5

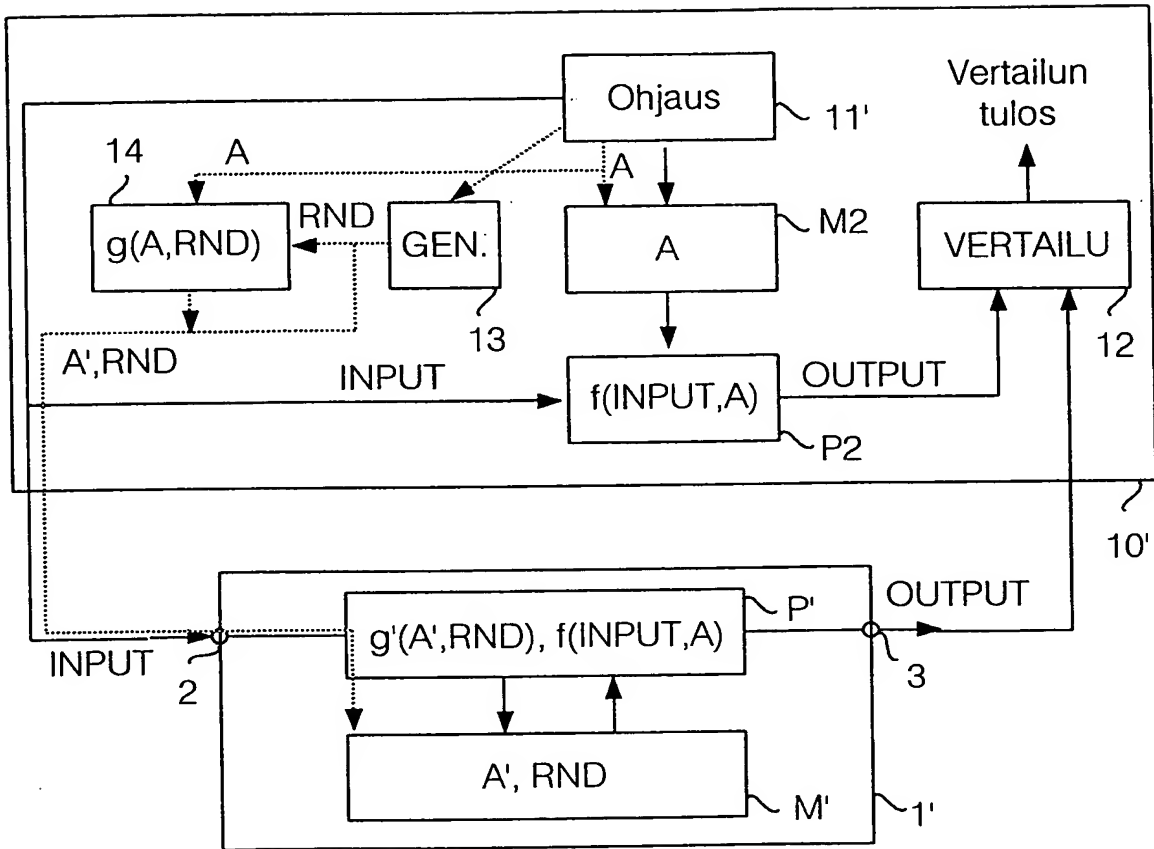


FIG. 6